IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
第 08-01-116 号
2008 年 1 月 7 日
独立行政法人 情報処理推進機構

# コンピュータウイルス・不正アクセスの届出状況［2007 年 12 月分］について

独立行政法人 情報処理推進機構（略称：IPA、理事長：藤原 武平太）は、2007 年 12 月のコンピュータウイルス・不正アクセスの届出状況をまとめました。

## 1．今月の呼びかけ

**今月の呼びかけ：「 そのメッセージに貴方は騙されていませんか？ 」**
**― セキュリティ対策ソフトの押し売り行為に注意！！ ―**

IPA には毎月、セキュリティ対策ソフトの押し売りのような行為に関する相談が相当数寄せられており、中には**「製品名称がローマ字表記であったため、もっともらしく感じて、安易にインストールしてしまった」**との相談例がありました。

以前からセキュリティ対策ソフトの押し売り行為は存在していましたが、従来は表示されるメッセージや製品名に英語表記が多かったことから、被害に遭うことを免れていたケースが多くありました。しかし、最近は表示されるメッセージも日本語になり、製品名も、(i) VirusuWadame（ウイルスはダメ）、(ii) KyoiKanshi（脅威監視）、(iii) KansenNashi（感染なし）などのローマ字表記の名称が使われているものが確認されています。一見、普通のセキュリティ対策ソフトと見間違うため、その結果、騙されてソフトをインストールしてしまい被害に遭うことが多いようです。

### (1)セキュリティ対策ソフトの押し売りとは

インターネットを利用していて突然、「あなたのパソコンからウイルスが発見されました」、「あなたのパソコンにはエラーが発生しています」といった内容のメッセージ画面が表示されて、それらの問題を解消するためには画面に表示されている「セキュリティ対策ソフト」の購入をするように勧められます。**実際には、ほとんどの場合、メッセージを偽って表示して、問題が無くても問題があるように見せかけて、セキュリティ対策ソフトの代金を支払わせようとする悪質な行為**です。代金を支払っても、そもそも問題がないわけですから、何の解決にもなりません。

例えば、利用者がホームページのバナー広告(ホームページ上にある画像広告)をクリックしたりすると、図 1-1 のようなページが表示され、図 1-1(a)のように、利用しているパソコンに本当に問題があるように見せかけた画像やメッセージが表示されます。

次に、問題の詳細を知りたい場合は、図 1-1(b)のボタンをクリックするように促します。実は、このボタンをクリックすると「セキュリティ対策ソフト」をダウンロードするように誘引されます。そのソフトは正規のセキュリティ対策ソフトとは機能が異なる事が往々にしてあります。

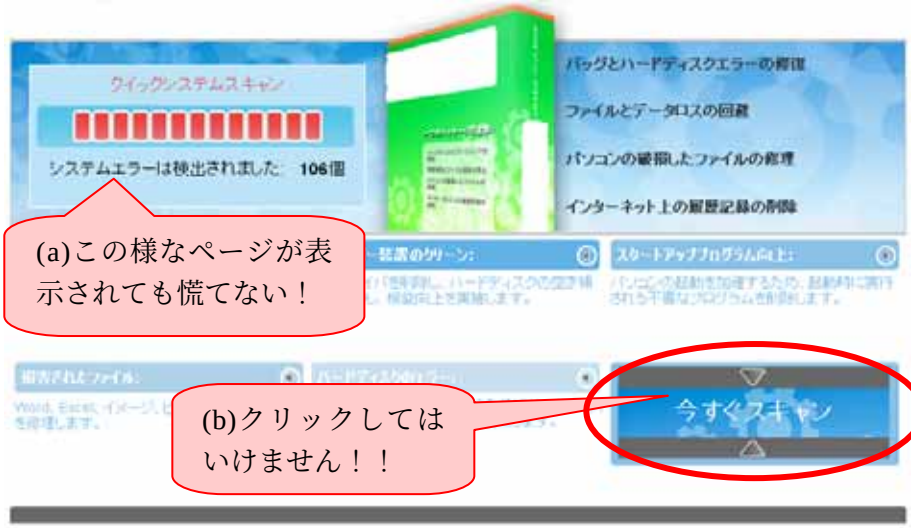


図 1-1:偽のメッセージ例

利用者がパソコンにインストールされた「セキュリティ対策ソフト」を、クレジット決済によって購入するまで、何度も購入を促す画面が表示し続けられたりします。

**(2)対応策**

この、「セキュリティ対策ソフト」の金額はわりと安価なことが多いです。何度も購入を促すメッセージ画面が表示され、そのメッセージを削除する方法もよくわからない場合に、利用者の中には小額なので支払ったほうが早いかなと考えてしまう場合があります。お金を支払っても購入を促すメッセージ画面が表示されなくなることはありません。**決してお金を支払わないでください。**

ホームページを閲覧中に**図 1-1 のようなメッセージ画面が表示されても、慌てて画面上のボタン等をクリックせずに、そのままブラウザを終了させる等をして無視することが最善の対策です。通常、正規のセキュリティ対策製品の製造・販売者からは、図 1-1 のようなメッセージ画面を一方的に送りつけることはありません。**

もし、この「セキュリティ対策ソフト」をインストールしてしまい、購入を促す画面が消えない場合は、その「セキュリティ対策ソフト」を**[スタート]->[コントロールパネル]->[プログラムの追加と削除]**から削除してください。

**(3)万が一の場合**

また、利用者のパソコンの動作が不安定（インターネットに接続出来ない、処理が遅くなる等）になる症状が表れる場合があります。このような症状が表れた場合には、以下のシステムの復元を実施して下さい。それでも症状が改善されない場合は、パソコンの初期化を実施して下さい。

**（a）システムの復元機能でシステムの状態を以前の正常な状態に戻す**

Windows には、任意の日を自動的に選んで、その日のパソコンのシステム状態を保存しており、パソコンの動作が不安定になったり、使用するのに支障が出る等の状態になった場合に、これらの保存された情報を基にして正常な状態に戻すことができる「システムの復元機能」があります。

この正常な状態が保存される任意の日は、ユーザが自分で設定することも可能となっています。

以下のマイクロソフトのホームページを参考にして、「システムの復元機能」を使用してシステムの状態を調子が良かった状態に戻す作業を行ってください。

ただし、選択した任意の日から現在までに、アプリケーションソフトウェアのインストール、アップデート等をした場合は、それらの情報は消えてしまいますので、システム復元後に再度実施してください。

なお、選択した任意の日から現在までに作成した文書や送受信したメール情報並びにホームページへのアクセス履歴やお気に入りは消えません。

「システムの復元のやり方」
http://www.microsoft.com/japan/windowsxp/pro/business/feature/performance/restore.mspx

**（b）パソコンの初期化**

パソコンを購入した時の状態に戻す作業を実施します。

実際の作業方法は、購入時に添付されている説明書に記載されている「購入時の状態に戻す」等の手順に沿って作業してください。

作業する前に重要なデータを外部媒体等にバックアップしてから作業を行って下さい。

※本作業によって生じたトラブル･損失･損害には、当機構では一切責任を負いかねます。あくまでも自己責任の下、自己判断で作業をしてください。

(ご参考)
IPA - パソコンユーザのためのウイルス対策 7 箇条
http://www.ipa.go.jp/security/antivirus/7kajonew.html
IPA - パソコンユーザのためのスパイウェア対策 5 箇条
http://www.ipa.go.jp/security/antivirus/spyware5kajyou.html

## 今月のトピックス

○ コンピュータ不正アクセス被害の主な事例（届出状況及び被害事例の詳細は、6 頁の「3.コンピュータ不正アクセス届出状況」を参照）

・ウェブサイトが改ざんされた
・オンラインゲーム上で使うアイテムが消失した

○ 相談の主な事例 （相談受付状況及び相談事例の詳細は、8 頁の「4.相談受付状況」を参照）

・個人使用パソコン内のデータが Winny ネットワークに流出しているらしい・・・
・ウイルスに感染した？

○ インターネット定点観測（詳細は、別紙 3 を参照）

IPA で行っているインターネット定点観測について、詳細な解説を行っています。

・2007 年の期待しない（一方的な）アクセスの状況について

## 2．コンピュータウイルス届出状況　－詳細は別紙１を参照－

ウイルスの検出数(※1)は、**約 34 万個**と、11 月の約 60 万個から約 4 割の減少となりました。
また、12 月の届出件数(※2)は、**2,239 件**となり、11 月の 2,351 件から 4.8%の減少となりました。

※1 検出数　：届出にあたり届出者から寄せられたウイルスの発見数（個数）
※2 届出件数：同じ届出者から寄せられた届出の内、同一発見日で同一種類のウイルスの検出が複数ある場合は、1 日何個検出されても届出 1 件としてカウントしたもの。
・12 月は、寄せられたウイルス検出数約 34 万個を集約した結果、2,239 件の届出件数となっています。

検出数の1位は、**W32/Netsky** で**約 30 万個 、2 位は W32/Stration** で**約 2.3 万個、3 位は W32/Mytob** で**約 1.1 万個でした。**

**ウイルス検出数　約34万個 (約60万個)　前月比 - 42.4%**

（注：括弧内は前月の数値）

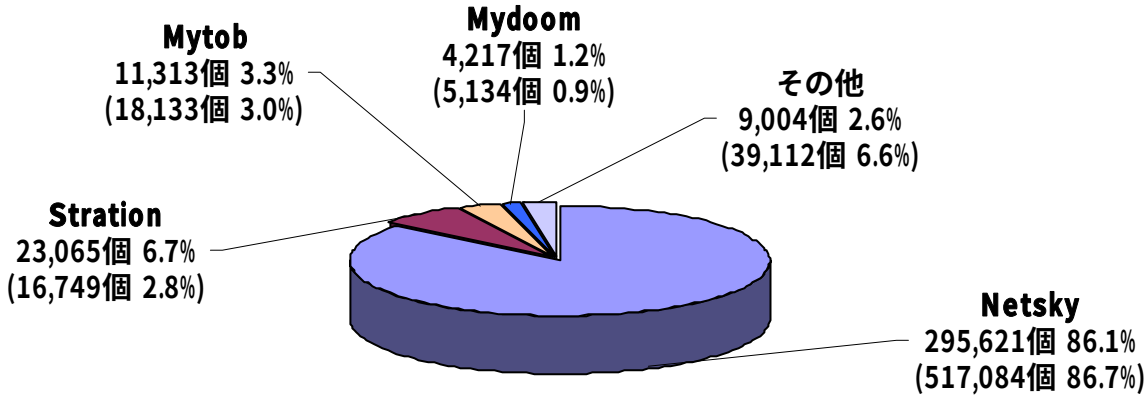



図 2-1

**ウイルス届出件数　2,239件 (2,351件)　前月比 - 4.8%**

（注：括弧内は前月の数値）

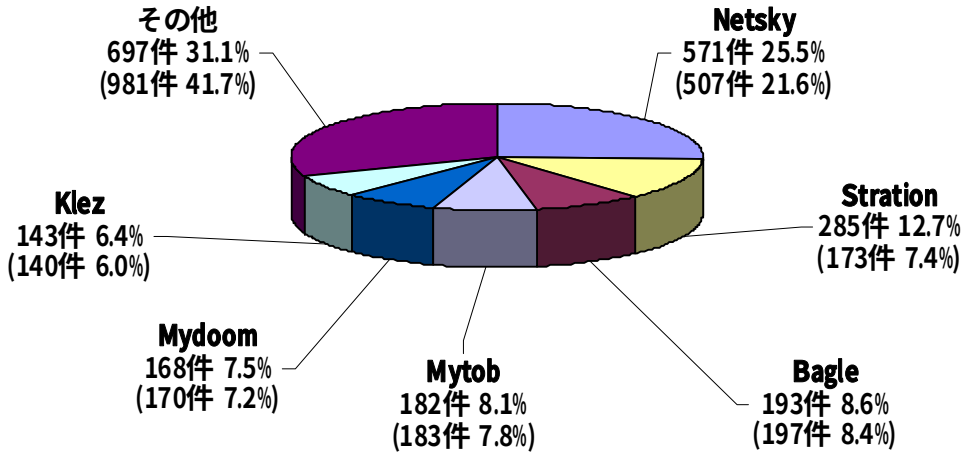



図 2-2

## 3．コンピュータ不正アクセス届出状況（相談を含む）　－詳細は別紙 2 を参照－

**不正アクセスの届出および相談の受付状況**

| | | 7月 | 8月 | 9月 | 10月 | 11月 | 12月 |
|---|---|---|---|---|---|---|---|
| **届出(a) 計** | | **10** | **16** | **10** | **10** | **15** | **14** |
| | 被害あり(b) | 8 | 13 | 8 | 9 | 11 | 7 |
| | 被害なし(c) | 2 | 3 | 2 | 1 | 4 | 7 |
| **相談(d) 計** | | **25** | **23** | **27** | **37** | **31** | **21** |
| | 被害あり(e) | 11 | 15 | 12 | 22 | 17 | 16 |
| | 被害なし(f) | 14 | 8 | 15 | 15 | 14 | 5 |
| **合計(a+d)** | | **35** | **39** | **37** | **47** | **46** | **35** |
| | 被害あり(b+e) | 19 | 28 | 20 | 31 | 28 | 23 |
| | 被害なし(c+f) | 16 | 11 | 17 | 16 | 18 | 12 |

### （1）不正アクセス届出状況

**12 月の届出件数は 14 件**であり、そのうち**被害のあった件数は 7 件**でした。

### （2）不正アクセス等の相談受付状況

不正アクセスに関連した相談件数は 21 件（うち 2 件は届出件数としてもカウント）であり、そのうち何らかの被害のあった件数は 16 件でした。

### （3）被害状況

被害届出の内訳は、**侵入 4 件、DoS 攻撃 1 件、その他（被害あり）2 件**でした。

侵入届出の被害は、ウェブサイトのコンテンツ改ざんが 4 件でした。そのうち 2 件は、そのサイトにアクセスしただけで、ウイルスをダウンロードさせられてしまうような悪質なサイトへ勝手にジャンプさせられる仕掛けを埋め込まれていたものです。また、フィッシング※に悪用するためのコンテンツを設置されていたものが 1 件ありました。

侵入の原因として、設定不備のものが 1 件ありました。他の 3 件は不明でしたが、サーバ OS その他アプリケーションのぜい弱性放置によるものと推測されます。

その他（被害あり）の被害として、オンライン RPG（ロールプレイングゲーム）上で自分のキャラクターのアイテムや所持金が消失していたものが 1 件ありました。

※フィッシング（Phishing）…正規の金融機関など実在する会社を装ったメールを利用して偽のウェブページに誘導し、それを見た利用者の ID やパスワードなどを詐取しようとする行為のこと。

## (4) 被害事例

### [侵入]

#### (i) ウェブサイトが改ざんされた

| | |
|---|---|
| **事例** | ・自社のサイトを閲覧した一般ユーザから、「サイトを開くと同時にウイルス対策ソフトがウイルス警告を発した」との通報があった。<br>・調査したところ、データベース内の多数のフィールドが、見覚えのない文字列【<script src="http://(省略).net/0.js"></script>】に改ざんされていた。<br>・このスクリプトによって、サイトを閲覧しただけでウイルスをダウンロードさせられてしまう仕掛けになっていた。 |
| **解説・対策** | データベースが改ざんされていたことから、ウェブサーバ上の**ウェブアプリケーションにぜい弱性があったため、SQL※インジェクション※攻撃で被害を受けた**ものと思われます。**先月に引き続き、同様の被害事例がいくつか寄せられており、なおも注意が必要です**。<br>**ウェブアプリケーションのぜい弱性を解消する**のはもちろんのこと、**ウェブサイトの改ざんチェックツールを利用する**など、多重防御に努めることが重要です。<br>(参考)<br>IPA - セキュアプログラミング講座(Web アプリケーション編)<br>http://www.ipa.go.jp/security/awareness/vendor/programmingv2/<br>IPA - 安全なウェブサイトの作り方 改訂第 2 版<br>http://www.ipa.go.jp/security/vuln/websecurity.html |

※SQL (Structured Query Language)…リレーショナルデータベースマネジメントシステム(RDBMS)において、データの操作や定義を行うための問合せ言語のこと。
※SQL インジェクション…データベースへアクセスするプログラムの不具合を悪用し、正当な方法以外でデータベース内のデータを閲覧したり書き換えしたりする攻撃のこと。

### [その他(被害あり)]

#### (ii) オンラインゲーム上で使うアイテムが消失した

| | |
|---|---|
| **事例** | ・自宅パソコンが故障したため、マンガ喫茶でオンライン RPG(ロールプレイングゲーム)をプレイ。<br>・後日、再度ログインしたところ、前にログアウトした場所とは違うところに自分のキャラクターが立っていた。<br>・不審に思い調査したところ、ゲーム内のキャラクターが持っていた武器などのアイテムや、ゲーム内通貨が消失していることを確認。<br>・ゲーム仲間がゲーム内で目撃した話によると、本人がプレイしていない時間帯に、何者かが本人になりすましてログインしていたようだ。 |
| **解説・対策** | この事例では、何らかの原因で**本人の ID とパスワードが盗まれてしまった**と思われます。マンガ喫茶やネットカフェなど公共の場に設置してあるパソコンには、悪意のある人間が**キーロガーなどのスパイウェア**を仕込んでいたりする場合もあります。また、**キー操作を背後から覗き見**されている場合もあります。**不特定の人間が操作するパソコンでは、会員制サイトへのログインや、ネットショッピング、ウェブメール送受信などは控えた方が無難です**。<br>(参考)<br>警察庁 - インターネット安全・安心相談<br>http://www.cybersafety.go.jp/ |

## 4．相談受付状況

12 月の相談総件数は **389 件**でした。そのうち**『ワンクリック不正請求』に関する相談**が **43 件**(11 月：264 件)と、激減しました。これは、11 月末にワンクリック不正請求業者が逮捕されたことが影響しているものと思われます。その他としては、**Winny に関連する相談**が **19 件**(11 月：31 件)、**『セキュリティ対策ソフトの押し売り』行為**に関する相談が **11 件**(11 月：14 件)などでした。

### IPA で受け付けた全ての相談件数の推移

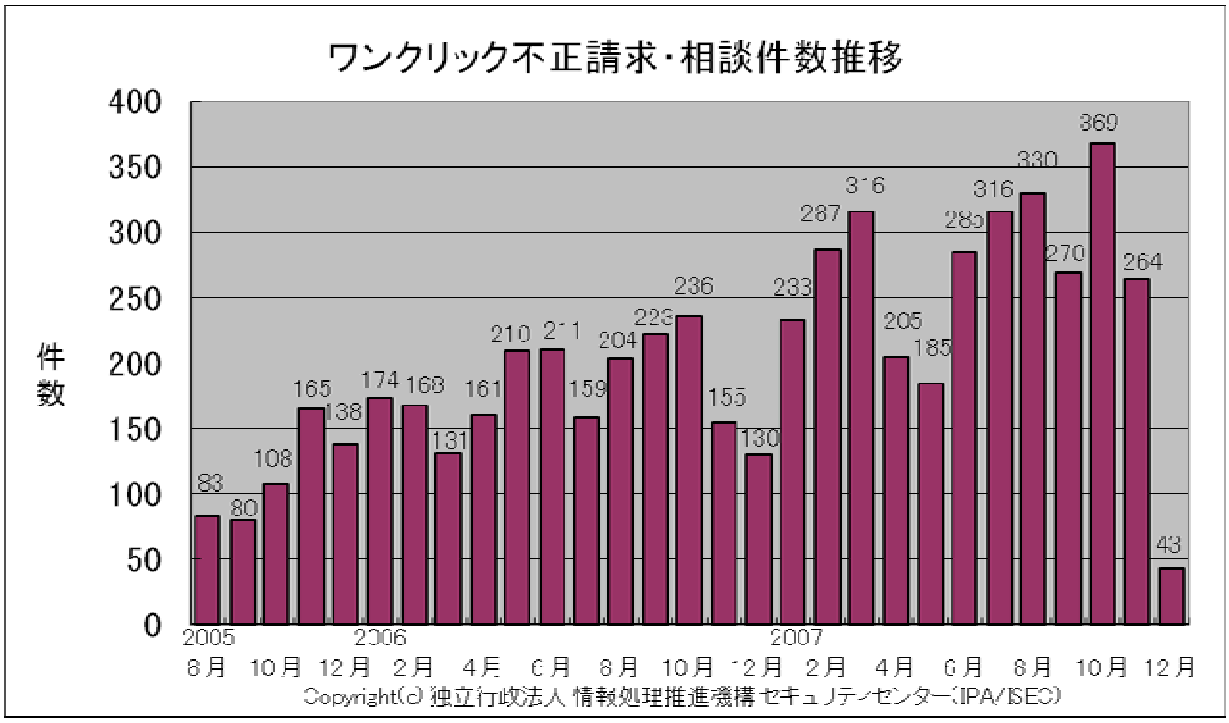
| | | 7月 | 8月 | 9月 | 10月 | 11月 | 12月 |
|---|---|---|---|---|---|---|---|
| **合計** | | **1162** | **1013** | **910** | **1128** | **911** | **389** |
| | 自動応答システム | 694 | 593 | 544 | 669 | 520 | 222 |
| | 電話 | 402 | 374 | 310 | 397 | 337 | 109 |
| | 電子メール | 65 | 43 | 55 | 57 | 52 | 56 |
| | その他 | 1 | 3 | 1 | 5 | 2 | 2 |

※ IPA では、コンピュータウイルス・不正アクセス、Winny 関連、その他情報セキュリティ全般についての相談を受け付けています。
メール：virus@ipa.go.jp（ウイルス）、crack@ipa.go.jp（不正アクセス）、
winny119@ipa.go.jp（Winny 緊急相談窓口）、isec-info@ipa.go.jp（その他）
電話番号：03-5978-7509（24 時間自動応答、ただし IPA セキュリティセンター員による相談受付は休日を除く月～金の 10:00～12:00、13:30～17:00 のみ）
FAX：03-5978-7518（24 時間受付）

※ 「自動応答システム」：電話の自動音声による応対件数
「電話」：IPA セキュリティセンター員による応対件数

※ 合計件数には、「不正アクセスの届出および相談の受付状況」における『相談[d] 計』件数を内数として含みます。

### （参考）ワンクリック不正請求相談件数の推移



主な相談事例は以下の通りです。

### (i)個人使用パソコン内のデータが Winny ネットワークに流出しているらしい・・・

| | |
|---|---|
| **相談** | 個人で使用しているパソコンで、Winny を利用している。会社の資料も保存している。ある日、某掲示板サイトで、パソコンのデスクトップ上のデータが流出しているという投稿を発見した。確認したところ、自分のパソコン内のデータだった。おそらく、ウイルスに感染してデータが流出したのだろう。どう対応したらよいか。 |
| **回答** | **会社のデータも流出している可能性が高い**ため、次のように行動しましょう。<br>(1)関係部署への報告<br>すぐ会社の緊急対応部署に連絡してください。あなたの上司で構いません。<br>**個人で対応しようとせず、会社の緊急対応部署の指示に従ってください**。<br>(2)パソコンの取扱い<br>情報漏えいした、「Winny を使っていたパソコン」をインターネットから切断してください。**絶対パソコン内の Winny を削除したり、ファイルを削除したりしないでください。流出したデータを特定するために必要です**。<br>その他の事項については、下記を参考にしてください。<br>(ご参考)<br>IPA - Winny による情報漏えいを防止するために<br>http://www.ipa.go.jp/security/topics/20060310_winny.html<br>IPA - 「情報漏えい発生時の対応ポイント集」<br>http://www.ipa.go.jp/security/awareness/johorouei/ |

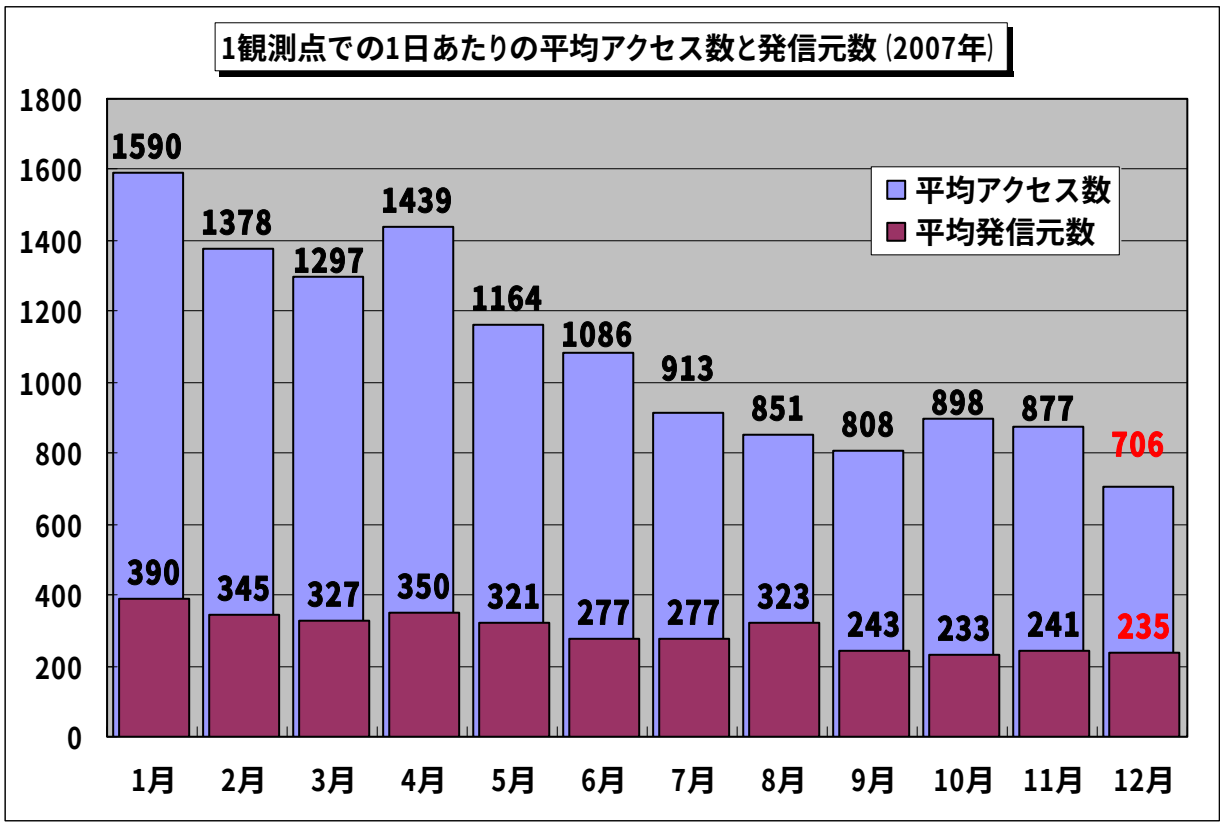
### (ii) ウイルスに感染した？

| | |
|---|---|
| **相談** | 2 週間くらい前から、下記の症状が出る。ウイルスに感染したのではないか。<br>・Windows Update しようとして、サイトにアクセスしてもページが表示されない<br>・ウイルス対策ソフトをダウンロードしようとしても、できない<br>・ウイルス対策ソフトベンダのサイトが閲覧できない(他のサイトは見られる)<br>・無償のオンラインウイルススキャンを実施しようとすると、関係ないショッピングサイトに飛ばされたり、「ページを表示できません」と出る |
| **回答** | 調査したところ、**正規のサイトにアクセスできなくするような仕掛けが施されていました**(hosts ファイルの改ざん)。ウイルスに感染した可能性が非常に高いので、**システムの復元を試みましたが、その機能自体が無効にされていました**。ウイルスによる影響が広範囲に渡っていると思われるため、**パソコンの初期化をお勧めします**。このように、ひとたびウイルスに感染すると復旧が非常に難しくなります。普段から、ウイルスに感染しないための予防策を実施することが重要です。<br>(ご参考)<br>IPA - パソコンユーザのためのウイルス対策 7 箇条<br>http://www.ipa.go.jp/security/antivirus/7kajonew.html |

## 5．インターネット定点観測での 12 月のアクセス状況

インターネット定点観測(TALOT2)によると、2007 年 12 月の期待しない（一方的な）アクセスの総数は、10 観測点で **218,942 件**ありました。1 観測点で 1 日あたり **235** の発信元から **706 件**のアクセスがあったことになります。

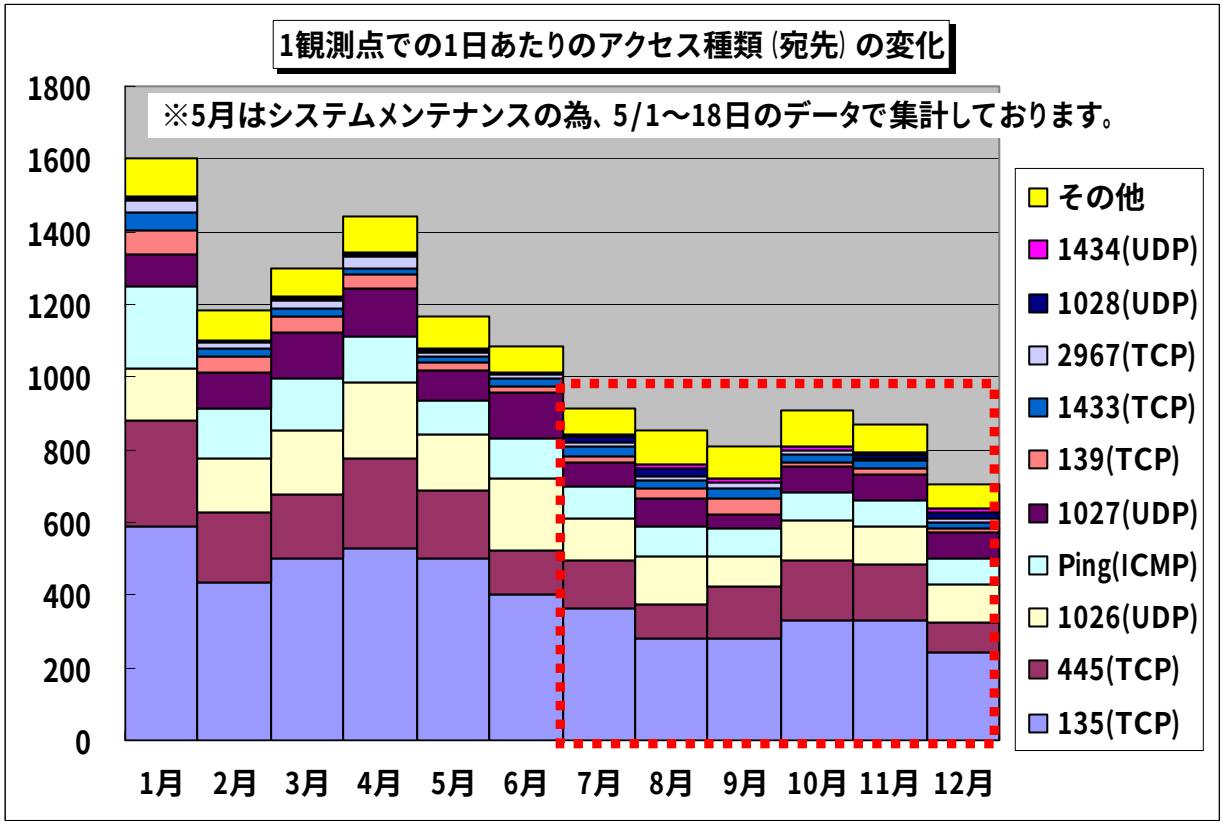
TALOT2 での 1 観測点の環境は、インターネットを利用される一般的な接続環境と同一なので、インターネットを利用される皆さんの環境へも同じくらいの一方的なアクセスがあると考えられます。言い換えれば、**あなたのコンピュータは、毎日、平均して、235 人の見知らぬ人(発信元)から、発信元一人当たり約 3 件の不正と思われるアクセスを受けている**と言うことになります。




【図 5-1　1 観測点での 1 日あたりの期待しない(一方的な)アクセス数および発信元数】

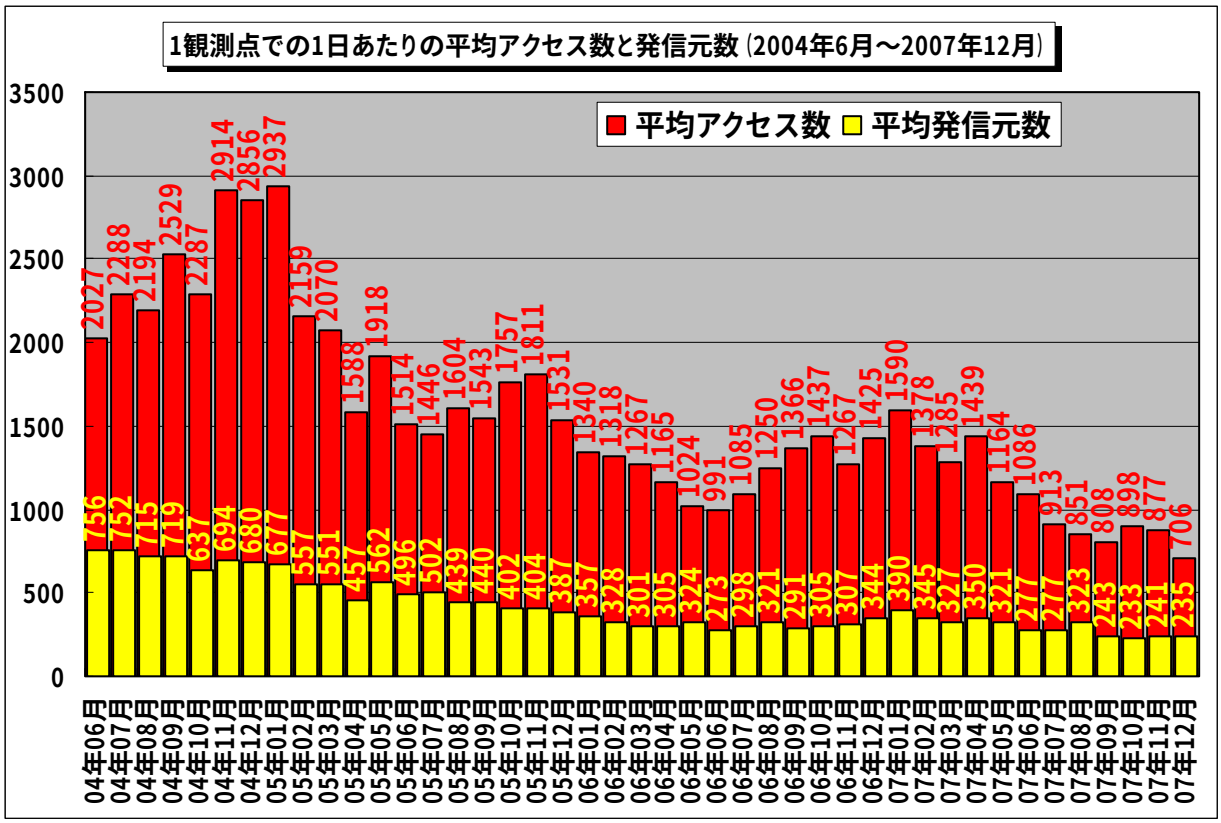
2007 年 1 月～2007 年 12 月までの各月の 1 観測点での 1 日あたりの平均アクセス数および、それらのアクセスの平均発信元数を図 5-1 に示します。この図を見ると、12 月の期待しない（一方的な）アクセスは 11 月よりも減少し、2007 年における 1 日あたりのアクセス数として最低となりしまた。ただし、全体的なアクセスの内容としては、定常化していると言えます。

2007 年の、毎月の 1 日あたりの期待しない（一方的な）アクセス状況は、6 月を境にアクセスの種類に関わらず全体的に少しずつ減少傾向にありました（図 5-2 参照）。




【図 5-2　1 観測点での 1 日あたりのアクセス種類（宛先）の変化】

また、定点観測を開始して以来、1 年を通した平均アクセス数でも過去最低となりました（図 5-3 参照）。




【図 5-3　2004 年 6 月～2007 年 12 月の 1 観測点での 1 日あたりの期待しない(一方的な)アクセス数および発信元数】

なぜアクセス数が少なくなったのかは定かではありませんが、要因を挙げるとすれば、

(1) Windows のぜい弱性を狙ったワームやウイルスによる、大量の感染被害が少なくなった
(2) 総務省･経済産業省連携プロジェクトである、サイバークリーンセンターが行なっているボット対策によるボットの駆除による効果
(3) 個人や企業の使用するコンピュータが、新しいマシンや新しい OS に入れ替わる事により、セキュリティ対策が向上する

などが考えられます。

(1)は、IPA に届けられる、コンピュータウイルス届出状況のウイルス届出数やウイルス検出数の減少からもうかがえますが、主に、各プロバイダで行なっている、迷惑メールやウイルスメールの対応も、感染被害の防止になっていると言えます。

(参考情報)
■ 2007 年コンピュータウイルスの届出状況について (PDF ファイル)
http://www.ipa.go.jp/security/txt/2008/documents/2007all-vir.pdf

(2) は、ボットウイルスからのアクセスと思われるものに対して、効果を上げていると思われます。サイバークリーンセンターでは、ボット駆除ツールの配布や、インターネットサービスプロバイダ (ISP) の協力の下、ボットに感染していると思われる顧客に対して、注意喚起メールの送信を行なったりしています。

(参考情報)
■ 総務省･経済産業省 連携プロジェクト Cyber Clean Center サイバークリーンセンター
https://www.ccc.go.jp/
■ ボットの駆除手順
https://www.ccc.go.jp/flow/index.html
■ 注意喚起活動について
https://www.ccc.go.jp/activity/index.html
■ ボット対策のしおり (PDF ファイル)
http://www.ipa.go.jp/security/antivirus/documents/3_bot_v5.pdf

(3) については、あくまでも推測ですが、2007 年 1 月に Microsoft Windows の新しい OS (Windows Vista) が発売されました。これに伴い、個人や企業が新しい OS のコンピュータに替える事により、古いコンピュータにボットウイルスなどが感染していた場合には、知らない間にボットウイルスなども一緒に破棄されてしまう形になります。

また、新しい OS のコンピュータには、最初からインストールされているウイルス対策ソフトが、期間限定であるとしても、最新の状態で機能する事も見逃せないのではないでしょうか。

以上の情報に関して、詳細はこちらのサイトをご参照ください。

別紙 3_インターネット定点観測（TALOT2）での観測状況について
http://www.ipa.go.jp/security/txt/2008/documents/TALOT2-0801.pdf

**『他機関・ベンダーの各種統計情報は以下のサイトで公開されています。』**

@police：http://www.cyberpolice.go.jp/
トレンドマイクロ株式会社：http://www.trendmicro.com/jp/
マカフィー株式会社：http://www.mcafee.com/japan/

**■お問い合わせ先**
独立行政法人 情報処理推進機構 セキュリティセンター
花村／加賀谷／宮本
Tel:03-5978-7527 Fax:03-5978-7518 E-mail:isec-info@ipa.go.jp